STATE of ARIZONA

Arizona Department Of Administration	**Agency STANDARD**	**TITLE: Acceptable Use of ADOA Information Resources**
	A800-M3-S02 Rev 0	**Effective Date: May 9, 2007** **Revision Date:**

1. AUTHORITY

1.1. The authority for this standard is based on the ADOA Policy A800 – Information Security.

2. PURPOSE

2.1. The purpose of this standard is to establish the responsibilities and restrictions by which every user of ADOA Information Resources is to comply.

2.2. This standard recognizes ADOA Information Security's (AIS) use of a Technology Infrastructure and Standards Assessment as the instrument for determining compliance to ADOA and Statewide IT Standards

3. SCOPE

3.1. This standard applies to all ADOA departmental business units, including divisions, contractors or other entities using departmental information technology resources and data.

3.2. The ADOA Director, in conjunction with the ADOA Information Security (AIS) Manager and the ADOA LAN Manager, are responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies, Standards and Procedures (PSPs).

4. DEFINITIONS AND ABBREVIATIONS

4.1. **Acceptable Use -** use of ADOA Information Resources that is authorized and meets ADOA policy and standards.

4.2. **Authorized Use -** use of ADOA Information Resources, that is:

4.2.4. performed according to designated duties listed within an employee's job description, as assigned by an employee's supervisor or as necessary to carry out the daily duties of the position;

4.2.5. required by a contractor to satisfy the services contracted by ADOA;

4.2.6. required by an outside organization under an inter-governmental agreement (IGA/ISA).

4.3. **Authorized Users –** all individuals approved to use ADOA Information Resources. These include full/part-time ADOA employees, temporary employees, contract employees and non-employees providing services or products to the agency and/or non-employees who are given access to information resources, information and data (e.g. suppliers on contract or outside organizations with intergovernmental service agreements (ISAs)).

4.4. **Information Resource -** any computing device, peripheral, software, local and wide area networks (LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including the Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth) information and data owned or controlled by the ADOA

5. STANDARD

5.1. ADOA Information Resources are intended to be used for state business purposes only. Limited use of ADOA Information Resources for personal needs is permitted as long as such use is consistent with ADOA policies and standards.

5.2. Authorized users will not use ADOA Information Resources for illegal, inappropriate or obscene purposes.

5.3. Authorized users will not connect any personal device to the ADOA network via an Ethernet port, switch, router, wireless or any other connection without prior written approval from ADOA Information Security Manager and the authorized users Division AD. Any personal device connected to the ADOA network is subject to inspection, seizure and destruction. The examples of devices include: personal computers, laptops, network storage devices, switches, hubs, wireless devices and any network device or any other personal item not specifically authorized by ADOA Information Security Manager and the authorized users Division AD.

5.4. Authorized users will not connect any personal device to an ADOA desktop or laptop, without prior written approval from ADOA LAN Manager and the authorized users Division AD. Any personal device connected to the ADOA network is subject to inspection, seizure and destruction. The examples of devices include: personal computers, laptops, PDAs, IPODs, MP3 Players, USB drive storage devices, cell phones, cameras, keyboards, mice, headphones or any other personal item not specifically authorized by ADOA LAN Manager and the authorized users Division AD.

5.5. Authorized ADOA LAN users will not install, load or execute in memory any software application or program without first requesting such through ADOA LAN. ADOA LAN will be responsible for approval of all ADOA LAN and desktop software purchases, installation and tracking of licenses. The ADOA CIO or their designee will approve all other software purchases.

5.6. Use of ADOA Information Resources, for political or personal gain is prohibited.

5.7. ADOA may restrict the use of specific Information Resources through additional standards. Divisions within ADOA may further restrict the use of their Information Resources.

5.8. All use of Information Resources for electronic communication must present ADOA in a manner that preserves the Agency's good reputation and high standards of professionalism. Any electronic communication that constitutes a significant representation of ADOA to the Public, must be approved by the appropriate Division Head or their designee**.** Consequently, any electronic communication discovered on a public ADOA site that is deemed inappropriate will be reported to ADOA Information Security and if necessary, the site will be disconnected until compliance can be achieved, with any incurred charges billed to the owning Division.

5.9. Distribution and retention of any information or data accessed through ADOA Information Resources must follow ADOA policy, ADOA Data Classification and Categorization Standard, Public Record Laws, and all state and federal regulatory requirements.

5.10. ADOA will have applications and systems in place that monitor and record computer usage. Every Internet/Intranet site or e-mail system accessed/visited is traced back to the originator. ADOA reserves the right to monitor all network traffic at any time, without prior notice or warning to the user. Anyone using ADOA Information Resources has **no expectation of privacy** in the use of these tools or content.

A. Examples of Improper Use:

1. Pursues illegal activities such as anti-trust or libel/slander.
2. Violates copyrights (institutional or individual), other contracts or license agreements (e.g. downloading or copying data, software or music that is not authorized or licensed).
3. Knowingly or with willful disregard, initiates activities that disrupt or degrade network or system performance, or wastefully uses the finite Information Resources.
4. Uses the ADOA Information Resources for fraudulent purposes.

5. Performs gambling activities or other illegal schemes (e.g. pyramid, chain letters, etc.).
6. Steals or destroys ADOA Information Resources or intellectual property.
7. Misrepresents another user's identification (forges or acts as), gains or seeks to gain unauthorized access to another user's account/data.
8. Obtains the passwords of other users or modifies or destroys another user's data.
9. Views, retrieves, saves or prints text or images of a sexual nature or containing sexual innuendo (e.g. accessing adult oriented sites or information via the Internet/Intranet).
10. Invades systems, accounts or networks to obtain unauthorized access for the purpose of damaging (hacking). This includes unauthorized scans, probes, or system entries.
11. Connects any unauthorized device to the ADOA network.
12. Copies, transfers or emails any ADOA data or information from the ADOA network, desktop computer, wireless device, storage device or media without the explicit permission of the authorized users supervisor or manager.
13. Intentionally intercepts and modifies the content of a message or file originating from or belonging to another person with the intent to deceive or further pursue other illegal or improper activities.
14. Knowingly circulates destructive programs into ADOA Information Resources (e.g., worms, viruses, parasites, Trojan horses, malicious code, e-mail bombs, etc.).
15. Uses ADOA Information Resources to conduct commercial or private business transactions, or supports a commercial/private business.
16. Promotes fundraising or advertising of non-ADOA organizations.
17. Generates or possesses material that is considered harassing, obscene, profane, intimidating or threatening, defamatory to a person or class of persons, or otherwise inappropriate or unlawful. This includes material that is intended only as a joke or for amusement purposes.
18. Discloses protected ADOA Information Resources (confidential or private) without proper authority.
19. Fails to comply with the instructions from appropriate ADOA management to discontinue activities that threaten the operation or integrity of ADOA Information Resources or those activities deemed inappropriate, or otherwise violate ADOA Policy and Standards.

Improper use of ADOA Information Resources is not limited to these examples.

5.7. Authorized users are responsible to protect and secure their ADOA Information Resources from unauthorized or improper use.

5.8. Users who encounter or receive any material that violates this Standard must immediately report the incident to their supervisors and notify the sender that such communication is prohibited under ADOA Policy and Standards.

5.9. When a user suspects that their account has been tampered with or compromised in any way, they are responsible for contacting the ADOA Help Desk to report the incident.

5.10. All authorized users are responsible for understanding and adhering to this standard and must sign and submit the attached Acceptable Use of ADOA Information Resources Acknowledgement Form to their supervisor.

5.11. If the authorized user is a state employee, the user's supervisor will forward the signed copy to the Division's personnel coordinator who will keep a copy and send the original to ADOA Human Resources.

5.12. If the authorized user is a contractor, the user's supervisor will forward the original signed copy to the Division's project manager to be filed.

6. STANDARD NON-COMPLIANCE

6.1. For non-compliance with this standard, all ADOA employees shall be subject to ADOA Human Resources progressive discipline, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.

6.2. Contractors and other authorized users will be held to contractual agreements.

7. REFERENCES

7.1. U.S. Code-Title 42-Subchapter XI-Part C-Sec 1320d-6-Wrongful disclosure of individually identifiable health information
7.2. ARS-13-2316 Computer tampering; venue; forfeiture; classification
7.3. ARS-13-2008. Taking identity of another person or entity; classification
7.4. ADOA Policy A800 – Information Security.
7.5. Statewide Policy – P800, IT Security

8. ATTACHMENTS

Acceptable Use of ADOA Information Resources Acknowledgement Form

ARIZONA DEPARTMENT OF ADMINISTRATION ACCEPTABLE USE OF ADOA INFORMATION RESOURCES ACKNOWLEDGMENT

I acknowledge that:

I have received, read, understand and agree to abide by the ADOA Standard A800-M3-S02 - Acceptable Use of ADOA Information Resources.

I understand that a copy of this signed Acknowledgement will be placed in my personnel file (project file in the case of a contractor).

_____ _____

Authorized User - Signature Supervisor - Signature

Date: _____

Authorized User (print): _____

Telephone No.: _____

Supervisor (print): _____

Division: _____

Note: ***A current signed copy of this form will be kept in the employee's personnel file, maintained by the ADOA Human Resources. All contractors are required to sign this form and a current copy will be filed with the contractor's ADOA Project Manager.***